



REC'D 13 JUL 2001

WIPO

PCT

# BREVET D'INVENTION

## CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

### COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

23 MAI 2001

Fait à Paris, le .....

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

**DOCUMENT DE PRIORITÉ****PRÉSENTÉ ET TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17(1) DE LA  
RÈGLE 17(1) DE LA  
RÈGLE 17(1) DE LA**

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 01 53 04 53 04  
Télécopie : 01 42 93 59 30  
<http://www.inpi.fr>

**Best Available Copy**

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W 01/99

<p>REMISE DES PIÈCES</p> <p>DATE <b>25 MAI 2000</b></p> <p>LIEU <b>75 INPI PARIS</b></p> <p>N° D'ENREGISTREMENT <b>0006693</b></p> <p>NATIONAL ATTRIBUE PAR L'INPI</p> <p>DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI <b>25 MAI 2000</b></p> <p><b>Vos références pour ce dossier</b> <b>FR 3897 JMD</b> <i>(facultatif)</i></p>		<p><b>1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE</b> À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</p> <p><b>BULL S.A.</b></p> <p><b>Monsieur Jean-Marc DIOU</b></p> <p><b>68, route de Versailles</b></p> <p><b>PC : 58D20</b></p> <p><b>78434 LOUVECIENNES Cedex</b></p>	
<p><b>Confirmation d'un dépôt par télécopie</b> <input type="checkbox"/> N° attribué par l'INPI à la télécopie</p>			
<p><b>2 NATURE DE LA DEMANDE</b></p> <p>Demande de brevet <input checked="" type="checkbox"/></p> <p>Demande de certificat d'utilité <input type="checkbox"/></p> <p>Demande divisionnaire <input type="checkbox"/></p> <p><i>Demande de brevet initiale</i> N° _____ Date ____/____/____</p> <p><i>ou demande de certificat d'utilité initiale</i> N° _____ Date ____/____/____</p> <p>Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i> <input type="checkbox"/> N° _____ Date ____/____/____</p>		<p><b>Cochez l'une des 4 cases suivantes</b></p>	
<p><b>3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b></p> <p><b>Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type internet, comprenant un segment de transmissions sans fil.</b></p>			
<p><b>4 DÉCLARATION DE PRIORITÉ</b> <b>OU REQUÊTE DU BÉNÉFICE DE</b> <b>LA DATE DE DÉPÔT D'UNE</b> <b>DEMANDE ANTÉRIEURE FRANÇAISE</b></p>		<p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p>Pays ou organisation _____ N° _____</p> <p>Date ____/____/____</p> <p><input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</p>	
<p><b>5 DEMANDEUR</b></p> <p>Nom ou dénomination sociale <b>BULL S.A.</b></p> <p>Prénoms _____</p> <p>Forme juridique <b>Société Anonyme</b></p> <p>N° SIREN <b>6 4 2 0 5 8 7 3 9</b></p> <p>Code APE-NAF <b>3 0 0 C</b></p> <p>Adresse <b>68, route de Versailles</b></p> <p>Rue _____</p> <p>Code postal et ville <b>78430 LOUVECIENNES</b></p> <p>Pays <b>France</b></p> <p>Nationalité <b>Française</b></p> <p>N° de téléphone <i>(facultatif)</i> <b>01.39.66.61.81</b></p> <p>N° de télécopie <i>(facultatif)</i> <b>01.39.66.61.73</b></p> <p>Adresse électronique <i>(facultatif)</i> <b>jean-marc diou@bull.net</b></p>		<p><input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</p>	

DÉPARTEMENT DES BREVETS


26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° . 1 / . 1  
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 V. 12-15-16

Vos références pour ce dossier <i>(facultatif)</i>		FR 3897 JMD	
N° D'ENREGISTREMENT NATIONAL		000 6693	
TITRE DE L'INVENTION (200 caractères ou espaces maximum)			
<p><b>Procédé et architecture de système de communication sécurisé entre deux entités connectées à un réseau de type internet, comprenant un segment de transmissions sans fil.</b></p>			
I.E(S) DEMANDEUR(S) :			
<p><b>BULL S.A.</b> 68, route de Versailles 78430 LOUVECIENNES</p>			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		Habert	
Prénoms		Michel	
Adresse	Rue	4, impasse J.H. Lartigue	
	Code postal et ville	38120 Saint-Egreve	
Société d'appartenance <i>(facultatif)</i>			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance <i>(facultatif)</i>			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance <i>(facultatif)</i>			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance <i>(facultatif)</i>			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		<p>Louveciennes, le 24 mai 2000</p> <p></p> <p>Jean-Marc DIOU (Mandataire Bull S.A.)</p>	

communiquer avec des couches de même niveau. Dans certaines architectures, l'une ou l'autre de ces couches peuvent être inexistantes.

Dans le cas d'un réseau de type Internet, les communications s'effectuent selon des protocoles, spécifiques à ce type de communications. 5 mais qui comprennent également plusieurs couches logicielles. Les couches sont au nombre de cinq, et de façon plus précise, en allant de la couche supérieure à la couche inférieure : la couche d'application ("http", "ftp", "e-mail", etc.), la couche de transport ("TCP"), la couche d'adressage de réseau ("IP"), la couche de liens de données ("PPP", "Slip", etc.) et la couche physique. Le 10 protocole de communication est choisi en fonction de l'application plus particulièrement visée : interrogation de pages "WEB" ("HTTP"), transferts de fichiers "FTP"), courrier électronique (e-mel, ou "e-mail" selon la terminologie anglo-saxonne), forums ou "news", etc.

Dans sa globalité, un réseau de type Internet comprend tout d'abord un 15 ou plusieurs réseaux de transmission de données proprement dits, éventuellement divisés en sous-réseaux. Ces réseaux comprennent notamment des canaux de liaison physique qui constituent le niveau le plus bas. Les communications peuvent être assurées par des liaisons à relativement bas débit : liaisons téléphoniques, ou des liaisons à haut ou très haut débit : fibres 20 optiques, faisceaux hertziens, liaisons satellites, notamment pour les artères principales. A ce ou ces réseau(x) sont connectés de nombreux systèmes, sous-systèmes, machines et/ou terminaux divers. La connexion peut être directe (à l'aide d'un modem, par exemple) ou indirecte, par l'intermédiaire d'un système dit "fire-wall" (ou "pare-feu"), d'un "proxy", ou par l'intermédiaire du système 25 informatique d'un fournisseur d'accès au réseau Internet (ou "ISP" selon la terminologie anglo-saxonne).

La gamme des entités connectées, dans l'art connu, peut aller des ordinateurs très puissants (par exemple du type dit "main-frame") jusqu'à des terminaux "légers", c'est-à-dire ne possédant que peu de ressources 30 informatiques propres, par exemple des terminaux dédiés, voire de simples terminaux lecteurs de carte à puce. Ces entités, que l'on peut appeler de façon générique "systèmes", disposent d'un système d'exploitation (ou "OS" selon la

Un premier besoin concerne la mobilité. On parle de "nomadisme" des utilisateurs. Ceux-ci disposant de terminaux eux-mêmes mobiles, tels des micro-ordinateurs portables, ils désirent pouvoir se connecter à n'importe quel endroit du réseau, sans contraintes excessives. Notamment, la migration d'un domaine à un autre devrait être transparente pour l'utilisateur. Il doit également pouvoir conserver son environnement habituel, par exemple conserver un accès à une liste de services auxquels il est abonné, gratuitement ou non, à un carnet d'adresses, etc. Les données caractérisant cet environnement peuvent être stockées dans un serveur éloigné auquel l'abonné peut accéder. Il peut encore les transporter avec lui, par exemple dans la mémoire d'une carte à puce.

Plus récemment, il a été proposé de connecter directement des téléphones mobiles, seuls ou combinés avec des appareils du type organisateur ou similaire, au réseau Internet. Cette connexion s'effectue physiquement par l'intermédiaire d'un réseau de transmissions sans fil, tel le réseau à la norme "Global System for Mobile communications (acronyme de "GSM"). Ce réseau est lui-même connecté au réseau Internet par l'intermédiaire de passerelles spécialisées ou "gateway" selon la dénomination anglo-saxonne.

Cette disposition est très avantageuse, car elle autorise une mobilité extrême. Il n'est plus nécessaire de disposer de points fixes pour se connecter au réseau Internet. *A priori*, la seule limite à cette mobilité résulte de la couverture territoriale, plus ou moins étendue, du réseau "GSM" d'un opérateur donné.

Cependant, il existe d'autres types de limitations dues à ce mode de transmission.

Une première limitation est relative à la bande passante. Dans l'état actuel des technologies, la vitesse de transmission est très faible : 9600 bits/s. Même dans le cas d'une simple ligne téléphonique filaire classique, la norme V90, par exemple, permet d'atteindre une vitesse maximale de 56000 bits/s. On peut obtenir des vitesses bien plus élevées si on fait appel à la technologie "ADSL" (470 kbits/s à 1 Mbits/s). En outre, les liaisons de type "RNIS", par câble ou satellites permettent de hauts ou très hauts débits. De nouvelles technologies sont en cours d'étude ou d'implantation, telle "GPRS"

ou autres moyens de transport, aux horaires de spectacles divers, etc., ou à l'affichage de vidéogrammes simples ou à des jeux peu gourmands en ressources informatiques.

5 Cependant, le recours à cette solution, pour des applications de type commerce électronique ou de type bancaire, par exemple, pose des problèmes relatifs à la sécurité, comme il va l'être montré ci-après.

En effet, un autre besoin qui se fait sentir, dans de nombreux domaines d'application est le niveau de sécurité offert par le système lors des transmissions entre deux entités.

10 Dans le cadre de l'invention, le terme "sécurité" doit être entendu dans un sens général. Il concerne tout d'abord la confidentialité : certaines données sont dites sensibles et ne doivent pas pouvoir être accessibles, à des entités non autorisées, personnes physiques ou applications logicielles. Pour ce faire, on a recours habituellement à diverses techniques de chiffrement. La sécurité  
15 concerne aussi les problèmes d'authentification entre parties, d'autant plus aigus que ces parties peuvent être mobiles sur le réseau Internet. L'authentification peut s'effectuer à l'aide de données d'identification (mots de passe) et/ou en ayant recours à la technique dite de certificats, en association avec des clés de chiffrement, par exemple stockées dans une carte à puce. La  
20 sécurité concerne aussi ce qui relève de l'intégrité des données transmises. On doit pouvoir s'assurer que les données reçues n'ont pas subi de modifications non désirées, que ce soit de manière accidentelle (défaillance des circuits de transmission par exemple) ou intentionnelles (malveillance, etc.). Pour ce faire, on peut mettre en œuvre des techniques de redondance et/ou des techniques  
25 de signature électronique (scellement).

Pour le réseau Internet "classique", une des techniques de sécurisation les plus utilisées fait appel à la technologie dite "SSL/TLS" ("secure Socket Layer/Transport Layer Security"). Cependant cette technologie n'assure qu'un niveau de sécurité minimal. Un niveau supérieur, d'ailleurs rendu obligatoire par  
30 la version dite "IPV6" des protocoles Internet (c'est-à-dire la version 6, la version actuellement utilisée étant majoritairement la version 4 ou "IPV4"), est assuré par le protocole de sécurité connu sous le sigle "IPSec". Il s'agit d'un

joue également un rôle d'interface assurant des conversions bilatérales "WAP" de ou vers "HTTP". Elle comprend notamment une couche logique de protocole "WAP" 110a et une couche logique de protocole "HTTP" 111a, complétée par une couche de sécurité "SSL/TLS" 111b, du côté "HTTP", et une couche (optionnelle) de sécurité "WTLS" 110b, du côté "WAP".

La passerelle 11 comprend enfin une interface 113 entre les deux séries de couches logiques destinées à effectuer la conversion bilatérale précitée. Or, précisément, cette interface 113, entre les protocoles de sécurité, "SSL/TLS" 111b et "WTSL" 110b introduit une faille de sécurité, ce qui crée une zone d'insécurité qui rend le concept dit "WAP gateway" qui vient d'être décrit incompatible, de façon pratique, avec le commerce électronique, les applications bancaires, et de façon plus générale avec toute application dite sensible exigeant un niveau de sécurité élevé.

Par contre, si l'on considère une station de travail 13, ou tout dispositif similaire sous le contrôle d'un usager  $U_2$ , connectée directement au réseau Internet  $R_I$ , les protocoles de communication utilisés entre cette station de travail 13 et le serveur 12 restent homogènes. Il n'existe pas de faille de sécurité intrinsèque au système. Il en aurait été de même, si la station de travail 13 avait été connectée au serveur 12 via un réseau intranet ou extranet.

L'invention vise à remplir les besoins qui se font sentir pour les communications via un réseau de type Internet, que ce soit un réseau de type classique ou un réseau mettant en œuvre la technologie "WAP", tout en palliant les inconvénients des dispositifs de l'art connu, et dont certains viennent d'être rappelés.

Pour ce faire, selon une première caractéristique, le concept précité dit "WAP gateway" est entièrement éliminé, ce qui permet de supprimer la faille de sécurité constatée au niveau de l'interface "WEB/WAP". La conversion "WAP/WEB" est effectuée directement au niveau des serveurs.

Selon une deuxième caractéristique, on attribue à chacune des entités devant être mise en relation une adresse dite permanente.

Selon une autre caractéristique, on adopte un mécanisme de sécurité de bout en bout, au niveau réseau, utilisable pour toute application de type

L'invention a encore pour objet une architecture de communication dans un ensemble de systèmes distribués pour la mise en œuvre du procédé.

L'invention va maintenant être décrite de façon plus détaillée en se référant aux dessins annexés, parmi lesquels :

- 5           - la figure 1 illustre schématiquement un exemple de réalisation d'un système de communication, selon l'art connu, comprenant un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP" ;
- la figure 2 illustre schématiquement un exemple d'architecture de système de communication via un réseau Internet et un réseau de communication sans fil mettant en œuvre la technologie "WAP", selon un mode de réalisation préféré de l'invention ;
- 10          - les figures 3 et 4 illustrent deux variantes de configuration de système serveurs selon l'invention ;
- les figures 5 et 6 illustrent une architecture de système permettant d'adresser directement une application logicielle hébergée par un système ;
- 15          - la figure 7 illustre de façon plus détaillée l'interconnexion de deux entités dans le système de la figure 2 ;
- 20          - la figure 8 illustre schématiquement une liaison sécurisée du type dit "tunnel" obtenue par le procédé selon l'invention ; et
- la figure 9 illustre un exemple d'architecture de système de communication sécurisée via un réseau Internet pour une application marchande en technologie dite "WAP".

25           Dans ce qui suit, sans en limiter en quoi que ce soit la portée, on se placera ci-après dans le cadre de l'application préférée de l'invention, sauf mention contraire, c'est-à-dire dans le cas d'un système de communication hybride comprenant un réseau Internet et, éventuellement, un réseau intranet, ainsi qu'un réseau de communication mobile, comportant un segment aérien, et

30           mettant en œuvre la technologie "WAP".

La figure 2 illustre de façon schématique un exemple d'architecture de système, désormais référencée 2, pour la mise en œuvre du procédé conforme



standards et "WAP". On peut aussi prévoir des systèmes dits "firewall" ou "pare-feu" (non représentés), par exemple inclus dans le serveur d'accès 22, isolant le réseau intranet *it* du monde extérieur, c'est-à-dire du réseau Internet *RI*.

5 Selon une caractéristique, également commune en soi à l'art connu, tout ou partie des machines ou systèmes connectés peut être mobile sur le réseau. Les autres utilisateurs devraient pouvoir adresser de façon transparente les machines qui ont migré. Aussi, au moins dans la version "IPV6" précitée, on prévoit un dispositif 23, connu généralement sous la dénomination anglo-saxonne "Home agent", ici connecté au réseau intranet *it*, permettant de gérer  
10 cette mobilité. Pour ce faire, un protocole dit "Mobile IP" est utilisé. Il permet de corréler une adresse temporaire attribuée à un système connecté avec une adresse permanente attribuée à l'entité qui lui est associée. Un utilisateur désirant adresser le système mobile ne manipule toujours que cette seule adresse permanente. Le protocole "Mobile IP" précité permet d'organiser une  
15 macro-mobilité. C'est le cas, par exemple, lorsque l'on change d'opérateur de réseau "GPRS".

Cet ensemble constitue un système distribué.

Jusqu'à présent, à l'exception de la structure de la passerelle 21, qui ne sert plus d'interface entre les protocoles "WAP/HTTP", l'architecture générale  
20 du système 2 qui vient d'être décrite est commune, en soi, à une architecture selon l'art connu (telle celle de la figure 1).

Selon une première caractéristique propre à l'invention, qui va être décrite en regard des figures 3 et 4, l'architecture des serveurs 3 est modifiée, de façon à ce que des conversions aux protocoles d'interfaces applicatives des  
25 serveurs "WEB" soient réalisées à l'intérieur de ceux-ci, et non plus au niveau de la passerelle 21, sous la forme de conversion de protocole de communication "WAP/HTTP". Le serveur 3 héberge donc une passerelle "WAP" avec un adaptateur d'interface applicative de serveur "WEB". Cette modification va permettre une sécurisation des transmissions, de bout en bout, transparente vis-  
30 à-vis des protocoles utilisés, "HHTTP", "WAP" ou autres (transmissions en mode paquet de données), ne présentant plus de faille de sécurité comme dans l'art connu, par la disparition de la fonction "WAP gateway". Elle permet enfin de ne

spécifiques 35. A titre d'exemple, on peut citer "TOMCAT", pour des serveurs de type "APACHE", sous système d'exploitation "LINUX" (tous ces termes correspondant à des marques déposées).

5 Selon la caractéristique avantageuse de l'invention qui vient d'être rappelée, le serveur "WAP" 30 dispose donc d'un adaptateur d'interface 32 qui permet aux applications écrites pour des serveurs "WAP" 30 d'utiliser les deux séries de mécanismes standards rappelés ci-dessus : applications "WAP" 36b et 36a respectivement.

10 Une deuxième variante de réalisation de l'invention est illustrée par la figure 4. Le serveur, ici référencé 3', comprend, comme précédemment, un serveur "WAP" 30 et un serveur "WEB" 31, ainsi que le module adaptateur d'interface 32. Cependant les applications présentes dans le serveur 3' sont uniquement des applications de type "WEB", référencées 37a à 37d, *a priori* écrites en langage "HTLM". Les applications "WEB" 37a et 37b correspondent  
15 aux applications "WEB" de mêmes références sur la figure 3, les applications 37c et 37d se substituant aux applications "WAP" 36a et 36b, respectivement. Des modules supplémentaires 38a et 38b sont intercalés entre les modules 33 et 34-35, d'une part, et les applications 38a et 38b, d'autre part. La fonction dévolue à ces module 38a et 38b est une conversion bidirectionnelle entre les  
20 langages "HTML" et "WML". De ce fait, les requêtes en provenance du serveur "WAP" 30 sont transmises via les modules 33 ou 34-35 aux convertisseurs 38a ou 38b, puis à une des applications "WEB" 37c ou 37d. Par contre, les requêtes en provenance du serveur "WEB" 31 sont transmises directement, des modules 33 ou 34-35 aux applications "WEB" 37a ou 37b. Le cheminement inverse est  
25 également vrai.

Selon une autre caractéristique du procédé de l'invention, une adresse permanente est attribuée aux utilisateurs ou à des applications clientes (par exemple  $U_1$  à  $U_4$ , figure 2), et aux applications serveurs (par exemple 36a-36b et/ou 37a-37b, figures 3 ou 4). De façon générale, on attribue une adresse  
30 permanente aux entités devant être connectées. Cette attribution peut être effectuée de façon dynamique.

Selon une troisième caractéristique du procédé d'adressage, les systèmes "réels" ou machines qui constituent, dans une configuration classique, des systèmes terminaux deviennent des systèmes intermédiaires. Ils constituent des nœuds des réseaux virtuels,  $SVN_1$  à  $SVN_n$ , et également des nœuds du réseau "réel", c'est-à-dire le sous-réseau Internet ou intranet  $SR_X$ . Les systèmes agissent en tant que passerelles qui interconnectent les nœuds des réseaux virtuels,  $SVN_1$  à  $SVN_n$ , au sous-réseau  $SR_X$ . Chaque système est également doté d'une adresse "IP".

On peut donc représenter un réseau virtuel système  $SVN_1$  associé à un système  $S_1$  de la façon illustrée par la figure 6. On constate qu'un système  $S_1$  constitue bien un nœud pour le réseau  $R_X$  et qu'il est associé, vu de ce réseau (c'est-à-dire de l'extérieur), à une première adresse  $IP_1$ , avec  $@IP_1:X,X_1$ ,  $X$  étant le préfixe attribué au sous-réseau  $SR_X$  et  $X_1$  l'adresse de  $S_1$  dans le sous-réseau  $SR_X$ .

On suppose que le réseau virtuel système  $SVN_y$  est constitué des deux serveurs référencés  $SV_A$  et  $SV_B$  qu'il héberge et du système  $S_1$  proprement dit. Vu du réseau virtuel système  $SVN_1$ , le système  $S_1$  est associé à une seconde adresse :  $IP_2$ , avec  $@IP_2:Y,Y_1$ ,  $Y$  étant le préfixe attribué au réseau virtuel système  $SVN_y$  et  $Y_1$  l'adresse de  $S_1$  dans le réseau  $SVN_y$ .

De même, les serveurs  $SV_A$  et  $SV_B$  sont associés à deux adresses,  $IP_A$  et  $IP_B$ , respectivement, avec  $@IP_A:Y,Y_A$ , et  $@IP_B:Y,Y_B$ ,  $Y_A$  et  $Y_B$  étant les adresses de  $SV_A$  et  $SV_B$ , respectivement, dans le réseau  $SVN_y$ .

Pour une description plus détaillée du mécanisme d'adressage, on pourra se référer avec profit à la demande de brevet français précitée, notamment à la figure 4 de cette demande qui illustre de façon détaillée l'architecture d'un système réel permettant l'adressage précité.

Dans le cadre de l'invention, les serveurs  $SV_A$  et  $SV_B$  peuvent être constitués par les serveurs "WAP" 30 et "WEB" 31 de la figure 3, le système réel  $S_1$  étant alors le système serveur 3.

Le procédé d'adressage selon la demande de brevet français précité, comme le procédé selon l'invention, restent compatibles avec le protocole Internet le plus couramment utilisé ce jour, c'est-à-dire la version "IPv4".

Selon le procédé de l'invention on implémente dans chaque système physique une pile protocolaire de communication comprenant successivement une pile "IPV6", 390 ou 44, incluant le protocole de sécurité "IPSec", 391 ou 45, et une pile "IPV4" 392 ou 46, respectivement pour le serveur 3 et les clients 4 ou 4'. Les piles "IPV4", 392 et 46, sont interfacées avec le réseau *R*. Les piles "IPV6", 390 et 44, sont interfacées avec les serveurs "WAP" 30 et "WEB" 31, côté serveur 3, et avec des clients "WAP" 42 et "WEB" 43, côté client 4.

Sur la figure 7, on a également détaillé les couches applicatives du client 4, qui présentent une grande symétrie avec celles du serveur 3. les clients, 42 et 42', peuvent être constitués par des navigateurs. Des associations de sécurité sont définies entre des utilisateurs ou des applications clientes et des applications serveurs. De façon avantageuse, un "triplet" identifie chaque association de sécurité :

- une adresse de destination des paquets de données ;
- un protocole de sécurité, de façon préférentielle le protocole dit "ESP" ("Encapsulating Security Payload" ou protocole d'authentification de données) est utilisé en mode tunnel ; et
- un paramètre index de sécurité ("Security Parameter Index" ou "SPI").

On constate que la sécurisation des transmissions, du fait que le chiffage et le déchiffage est réalisé en amont des couches d'adresses "IPV4", dans chaque entité à mettre en relation, on obtient bien la sécurisation transparente désirée, de bout en bout. On ne constate plus de faille de sécurité lors du cheminement des données, même si un segment du réseau est du type à transmissions sans fil.

Le schéma équivalent à l'architecture représentée par la figure 7 est celui illustré par la figure 8. Le canal de transmission peut en effet être représenté symboliquement sous la forme d'un câble blindé ou "tunnel" mettant en liaison deux entités, arbitrairement référencées  $E_1$  et  $E_2$ , auxquelles les adresses permanentes respectives  $@IP_{E1}$  et  $@IP_{E2}$  ont été attribuées. Il s'agit, soit d'adresses "IPV6", soit d'adresses compatibles "IPV6" si le réseau est au protocole "IPV4".

"tunnel" (figure 8), une authentification de la source d'information (une adresse "IPV6" permanente), en l'occurrence l'identification de l'utilisateur, est présente dans chaque paquet de données et chiffrée. En outre, la source de données est authentifiée et, dans ce cas, représente l'utilisateur. Cette identification est  
5 utilisée pour construire un contexte de sécurité utilisé lui-même par l'application ou, mieux, par le contenant de l'application pour effectuer un contrôle d'accès pour des contrôles d'autorisation.

Pour fixer les idées, on va maintenant décrire un exemple d'architecture de système de transmission, mettant en œuvre les dispositions de l'invention,  
10 adaptée à une application marchande mobile sécurisée, empruntant un tronçon de réseau de radio-transmission par paquets, par exemple du type "GPRS".

La figure 9 illustre schématiquement une telle architecture, référencée 2". Les éléments communs aux figures précédentes portent les mêmes références et ne seront re-décrits qu'en tant que de besoin.

15 Comme précédemment, le système 2", dans sa globalité comprend des terminaux mobiles, dont un seul, 20 sous le contrôle de l'utilisateur  $U_1$ , a été illustré. Ce terminal mobile 20 est connecté au tronçon de réseau sans fil  $RTT$ , puis via la passerelle 21 au réseau terrestre public  $RT$ , au réseau Internet  $RI$ . Un serveur, par exemple du type 3 de la figure 3, hébergeant au moins une  
20 application marchande par exemple l'application 36a, en technologie "WAP", est connecté au réseau Internet via le réseau Intranet  $it$  et le serveur d'accès 22. On a également représenté un terminal "WEB" 24 connecté au réseau intranet  $it$ . Ce terminal est similaire à la station 24 de la figure 2.

On n'a pas représenté les piles protocolaires d'adressage et "IPSec"  
25 (voir figure 7) permettant d'attribuer des adresses "IPV6" et d'effectuer les opérations nécessitées par le protocole "IPSec".

L'architecture qui vient d'être décrite permet d'établir un lien logique //s entre l'utilisateur  $U_1$  et l'application marchande "WAP" 36a, sécurisé de bout en bout, ce malgré le fait qu'il emprunte un segment de réseau sans fil.

30 A la lecture de ce qui précède, on constate aisément que l'invention atteint bien les buts qu'elle s'est fixés.

## REVENDEICATIONS

1. Procédé de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisé en ce que lesdites première et seconde entités sont constituées par une pièce de logicielle (36a-36b, 37a-37b) hébergée dans un desdits systèmes (3, 3') connectés audit réseau de type Internet ( $R/I$ ,  $R$ ) et/ou un utilisateur ( $U_1$ ) desdits systèmes connectés (4, 20), en ce que ledit premier système (4, 20) fonctionne en mode dit client et ledit second système (3, 3') fonctionne en mode dit serveur, en ce qu'il comprend une étape d'attribution, sur ledit ensemble de systèmes, d'une adresse permanente de type Internet, du type dit "IP", à chacune desdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d), en ce qu'il est implanté dans ledit second système formant serveur (3, 3') au moins une pièce de logiciel formant serveur (30, 31) et offrant les services d'au moins une application (36a-36b, 37a-37d) à ladite première entité ( $U_1$ ), et en ce qu'il est implanté dans lesdits premier (4, 20) et second (3, 3') systèmes une pile protocolaire de communication comportant au moins une couche (45, 391) pour l'exécution d'une étape de chiffrement, en mode bout en bout, conforme à un protocole de sécurisation déterminé, de données échangées entre lesdites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d).
2. Procédé selon la revendication 1, caractérisé en ce que lesdites adresses permanentes "IP" attribuées aux dites entités interconnectées ( $U_1$ , 36a-36b, 37a-37d) sont conformes au protocole d'adressage de type Internet "IPV6".
3. Procédé selon la revendication 2, caractérisé en ce que lesdites communications sur ledit réseau de type Internet ( $R/I$ ,  $R$ ) s'effectuant selon le protocole d'adressage de type Internet "IPV4", il comprend l'implantation dans lesdits premier (4, 20) et second (3, 3') systèmes d'une couche protocolaire

(35) d'adaptation bilatérale d'interface de structures permettant de supporter des interfaces applicatives (33) utilisées par les serveurs de type "WEB".

5 9. Procédé selon la revendication 7, caractérisé en ce qu'il comprend l'implantation dans ledit premier système (4, 20) d'une pièce de logiciel constituant un client et en ce que cette pièce de logiciel est un navigateur de type "WAP".

10 10. Procédé selon la revendication 1, caractérisé en ce que ledit premier système étant un système mobile (25), il comprend l'attribution au dit premier système (25) d'une adresse temporaire, en ce qu'il comprend une étape de dialogue entre ledit premier système (25) et un organe d'un type dit "home agent" (23), connecté au dit réseau de type Internet (*it*), permettant de corréler à chaque instant ladite adresse permanente, attribuée à ladite première entité ( $U_3$ ), avec ladite adresse temporaire, selon un protocole dit "mobile IPV6 protocol".

15 11. Architecture de système de communication sécurisé entre des première et seconde entités interconnectées via un réseau de type Internet, lesdites entités étant associées à des premier et second systèmes de traitement informatique de données parmi un ensemble de systèmes distribués connectés au dit réseau de type Internet, caractérisée en ce que le dit  
20 premier système (4, 20) est un système fonctionnant en mode dit client et ledit second système (3, 3') un système fonctionnant en mode dit serveur, en ce que lesdites première et seconde entités sont des pièces de logicielles (36a-36b, 37a-37d) hébergées dans lesdits premier (4, 20) et second (3, 3') systèmes et/ou un utilisateur ( $U_1$ ) desdits systèmes connectés, en ce lesdites  
25 entités ( $U_1$ , 36a-36b, 37a-37d) sont associées à des adresses permanentes de type Internet, du type dit "IP", en ce que ledit second système (3, 3') formant serveur comprend au moins une pièce de logiciel (31) formant serveur (30, 31) et offrant les services d'au moins une application (36a-36b, 37a-37d) à ladite première entité ( $U_1$ ), et en ce que lesdits premier (4, 20) et  
30 second (3, 3') systèmes comprennent une pile protocolaire de communication

"WAP" (30) et un deuxième module (32) formant une interface unifiée entre ledit serveur "WAP" (30) et au moins une application (36a-36b, 37a-37d) offrant ses services à ladite première entité ( $U_1$ ), de manière à ce que ledit serveur "WAP" (30) soit intégré en tant que serveur "WEB" dans ledit système serveur (3, 3').

5

**16.** Architecture selon la revendication 15, caractérisée en ce que ledit second système (3, 3') comprend au moins un module supplémentaire (38a-38b) de conversion bilatérale de paquets de données de structures conformes aux dits protocoles "WEB" ou "WAP".

10

**17.** Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile (20, 4) à la norme dite "GSM", en ce qu'il comprend un navigateur de type WAP constituant un client, et en ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

15

**18.** Architecture selon la revendication 15, caractérisé en ce que ledit premier système est un terminal de téléphonie mobile à la norme dite "GPRS" et en ce qu'il comprend un navigateur de type Internet constituant un client, et en ce qu'il comprend un écran de visualisation pour l'affichage de pages en langage du type dit "WML".

20



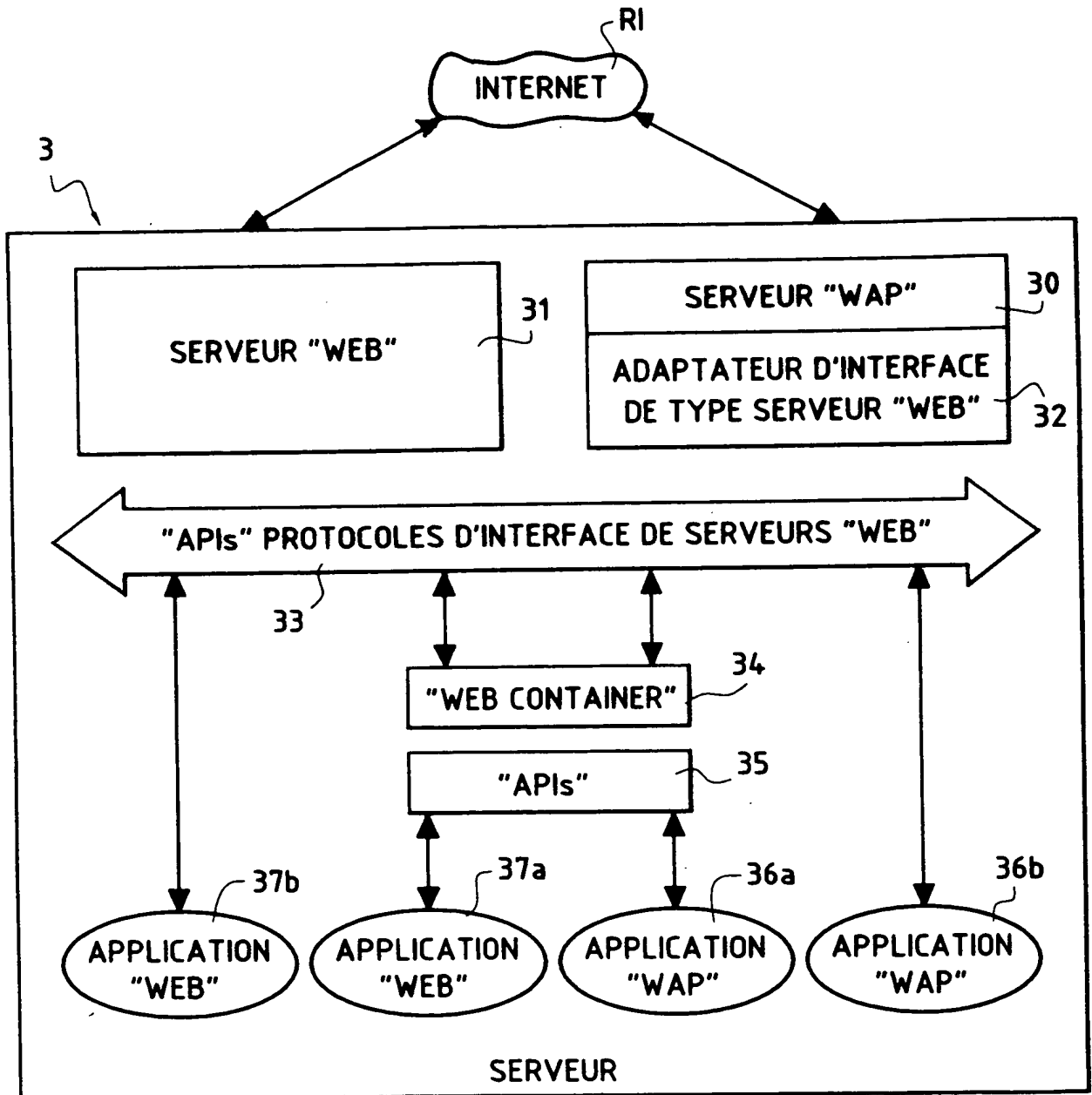


FIG.3

FIG.5

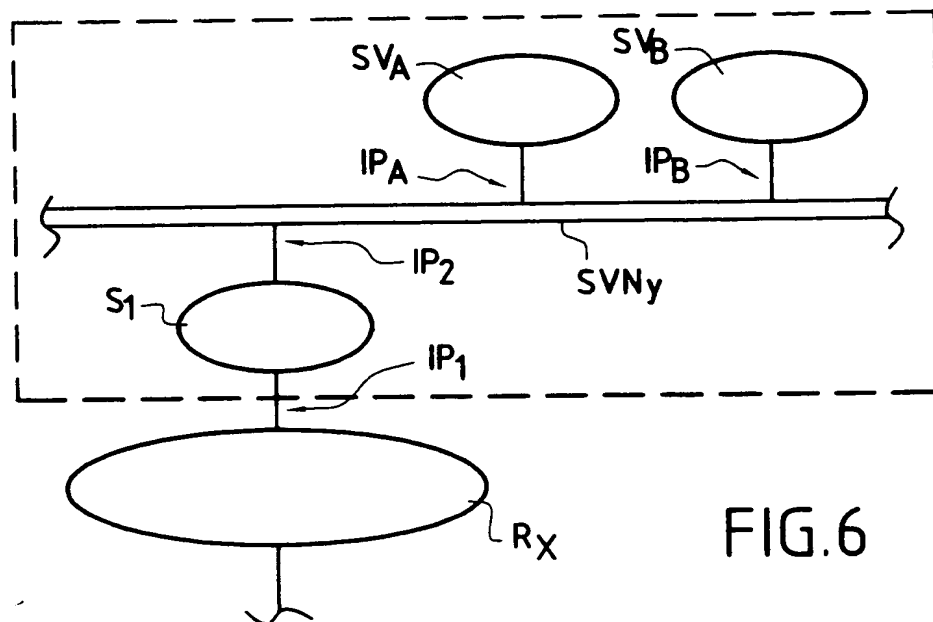
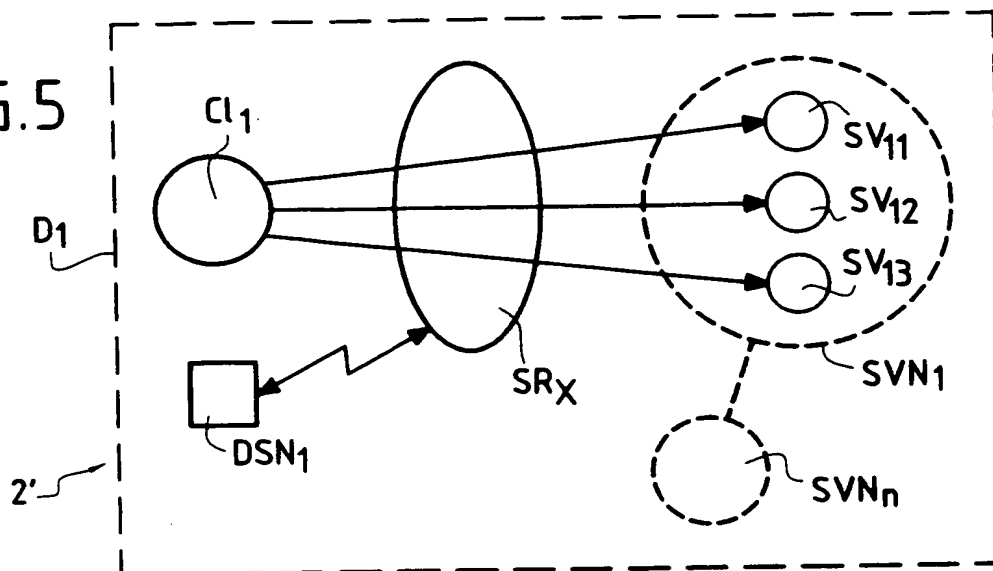


FIG.6

FIG.8

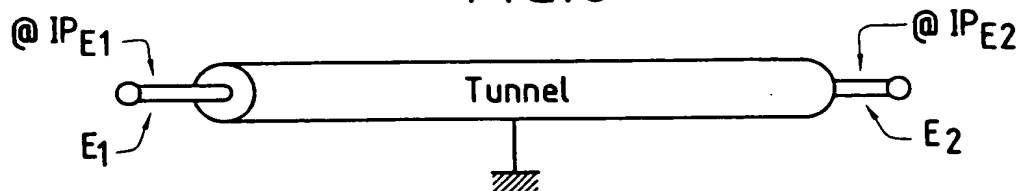
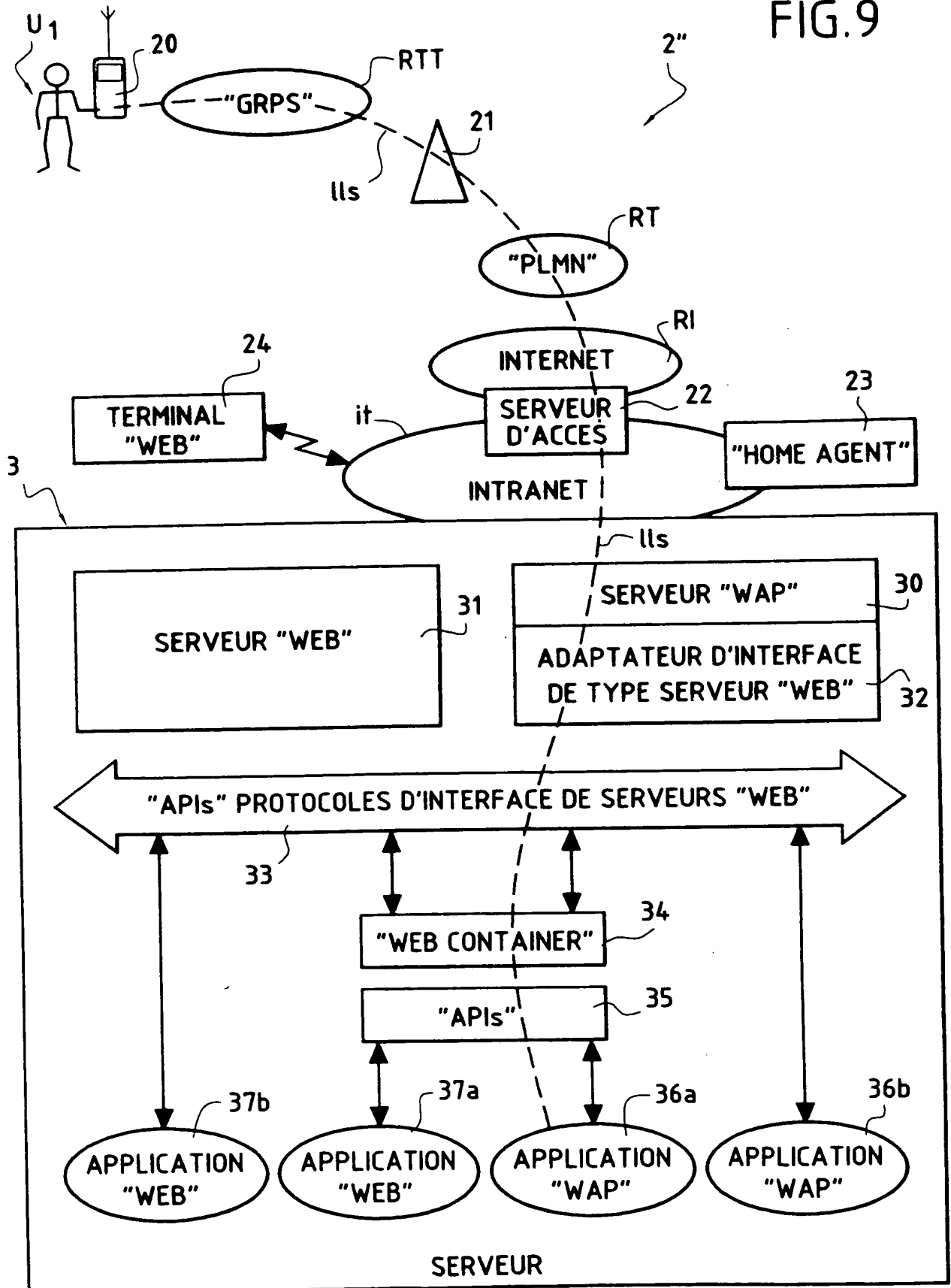


FIG. 9



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☒ OTHER: pages are skipping

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**